REMARKS

Applicant respectfully requests reconsideration and allowance in view of the foregoing amendements and the following remarks. Applicant notes that claims 1, 6, 8 and 14 have been amended. Thus, claims 1-14 are pending in the application.

Section 103 Rejections:

In the Office Action, claims 1-14 were rejected under 35 U.S.C. 103(a) as being unpatentable over Zheng ("The SPEED Cipher") and Sprunk (US Patent No. 5,404,402).

With regard to independent claim 1, Applicant notes that this claim has been amended to more particularly recite that the at least one cryptographic sub-operation is performed using at least one of the data x_i, k_i and/or the result or at least one intermediate result y_i that is bit-wise complemented to $\bar{x}_i$, $\bar{k}_i$ and/or $\bar{y}_i$ or not, depending on a control signal r_i which is based on random numbers. The Office Action acknowledges that Zheng fails to teach a bit-wise operation depending on a control function ri based on a random number, and instead relies on Sprunk. Sprunk, however, generally describes a clock signal that is modulated by a random function to provide an unpredictable stream of clock pulses. In this context, the modulated clock signal described in Sprunk causes the microprocessor to perform operations (or not) depending on the unpredictable stream of clock pulses. However, this modulated clock signal only controls when the operations are performed and does not control how the operations are performed. Applicant, accordingly, respectfully submits that the Sprunk fails to teach or suggest that at least one cryptographic sub-operation is performed using data and/or a result that is bit-wise complemented or not, depending on a control signal r_i which is based on random numbers as recited in claim 1. Embodiments of claim 1 provide certain advantages over Zheng and Sprunk by randomly switching between performing cryptographic sub-operations on the original data or the bit-wise complemented data to inhibit Differential Power Analysis. Therefore, because Zheng and Sprunk, alone and in combination, fail to teach or suggest claim 1, Applicant respectfully requests that the Section 103(a) rejections with respect to claim 1 and all claims dependent thereon be withdrawn.

With regard to independent claim 8, Applicant notes that this claim has been amended to recite that the controllable inverter (18 to 28; 30) either, in dependence on the control signal r_i, converts the bit series x_i, k_i or y_i into their bit-wise complement $\bar{x}_i$, $\bar{k}_i$ and $\bar{y}_i$, respectively, or leaves them unchanged for use in performing the at least one cryptographic operation. Because claim 8 has been amended to recite subject matter similar to claim 1, Applicant respectfully

submits that claim 8 defines over the cited art for reasons similar to those discussed above with respect to claim 1. Therefore, Applicant respectfully requests that the Section 103(a) rejections with respect to claim 8 and all claims dependent thereon be withdrawn.

In view of the foregoing amendments and remarks, Applicant respectfully submits that claims 1-14 are in condition for allowance. Applicant, accordingly, respectfully requests that a notice of allowance be issued with respect to claims 1-14.

Please charge any fees which may be required, except the issue fee, or credit any overpayment to Deposit Account No. 14-1270.

Date: April 5, 2003

Respectfully submitted,

By _____

Kevin Simons, Reg. No. 45,110
(408) 474-9075
Philips Electronics North America
1109 McKay Drive; Mail Stop SJ41
San Jose, CA 95131 USA